(19) JAPAN PATENT BUREAU (JP) (11) Publication No.: H4-297157

(12) OFFICIAL GAZETTE LAID-OPEN PATENT (A)

(43) Date of laying open:
October 21, 1992

(51) Int. Cl.[5]: ID Code:	Intraoffice No.:	FI: Technology display area:
H 04 L 9/28		
G 09 C 1/00	7922-5L	
H 04 K 1/00	7117-5K	
	7117-5K	H04L 9/02 A

Request for exam.: None
No. of Claims: 2 (Total of 4 pages)

(21) Application No.: H3-49700

(22) Date of Application: 3/14/1991

(71) Applicant: 000006013
MITSUBISHI DENKI K.K.
2-3, 2-Chome, Marunouchi,
Chiyoda-ku, Tokyo-to

(72) Inventor: M. MINAKI
c/o Mitsubishi Denki K.K.
Kamakura Plant,
325, Kamimachiya, Kamakura-shi

(74) Agent: M. TAKADA, Patent Agent
(and 1 other)

(54) Title: DATA CIPHER DEVICE

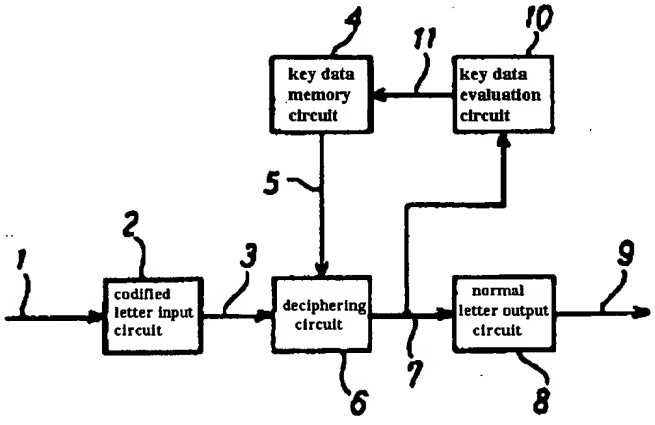
(57) Abstract:

Objective:

For the secret key cipher communication system, when the sender and recipient are separated over a long distance and the only means to send key data is via a route that can be intercepted by a 3rd party; to make reading of key data sent to a 3rd party and reading of the renewal time of the key data difficult.

Composition:

The specific feature of normal data, which is read by a data cipher device on the recipient's side, is detected, renewal of the key data is notified from sender to recipient, and the recipient's side is advised of the renewed key data and renewal time by extracting the key data itself, at the same time, from the said features.



PATENT CLAIMS

Claim 1

For the data cipher device that receives a cipher which is coded by a secret key cipher method and produces normal data by deciphering said data;
a data cipher device which has a coded data input circuit that receives coded data,
a key data memorizing circuit that memorizes the cipher key data which is necessary for deciphering of coded data,
a cipher deciphering circuit that receives key data from the key data memorizing circuit and coded data output from the said coded data input circuit and that outputs the deciphered result as normal data,
a normal data output circuit that receives normal data from the cipher deciphering circuit and outputs the said data, and
a key data evaluation circuit that evaluates the renewal time of the key data by receiving normal data from the said cipher deciphering circuit and supplies the said evaluation result to the said key data memorizing circuit.

Claim 2

Data cipher device of Claim 1, which has the following circuits as the key data judging circuit; a "No. of 1's" counting circuit that receives normal data composed of "1's" and "0's", which are split into blocks of a set bit and counts the number of "1's" contained in each normal data block,
a latching circuit with n steps (n is an integer) that memorizes the number of "1's" in the multiple input normal data block by the latching count values of the said "No. of 1's" counting circuit in sequence,
a count-value collating circuit that adds up the output of the said latching circuit with n steps and generates a count-value agreement signal when the said addition agrees with a previously set value, and
a renewal key data editing circuit that assumes an "unable" condition by receiving a count-value match detection signal from the said count-value collating circuit, and that edits the latched output of the said n-stepped latching circuit and generates new key data from the edited result.

DETAILED EXPLANATION OF THE INVENTION

[0001]

Area of industrial application

This invention relates to a cipher deciphering device for the cipher communication system that uses multiple key data.

[0002]

Conventional technology

Generally, in the field of digital communication, a signal from the data source is converted to a binary numerical row composed of 2 values, i.e., "1's" and "0's" and a transfer signal is modulated with such 2 values for radio or wired transmission to the target location. The signal from the data source can be word characters, voice or image, etc., and these signals are easily intercepted by a 3rd party. For transmission of data via a route that can be intercepted by a 3rd party, the data is coded for confidential data and the recipient deciphers such data. This is the so-called cipher communication system.

[0003]

Cipher communication systems are based on various principles and a popular one is the secret key cipher method. This method can transpose type where the sequence of data such as characters, etc., is transposed, or the letter-conversion type, where data of characters, etc., is switched to other characters, etc. With these manipulations, processed data cannot be deciphered by a 3rd party who has no knowledge of the nature of the process. Also, it is only decipherable by a recipient who has knowledge of the nature of the process. Therefore, a collation table, for transposition or switching of characters, which is known by the sender and the recipient must be protected from a 3rd party. The collation table is called a key, so the above method is called a secret key cipher method.

[0004]

Figure 3 is an example of a conventional cipher deciphering device for the secret key cipher method and, in the figure, 1 is an input coded letter, 2 is a coded letter input circuit, 3 is a coded letter, 4 is a key data memory circuit, 5 is the key data, 6 is a deciphering circuit, 7 is a normal letter, 8 is a normal letter outputting circuit and 9 is the normal letter output.

[0005]

Next, the function of the invention is explained. Input coded letter 1 is received by coded letter input circuit 2 and is input to deciphering circuit 6 as a coded letter 3. On the other hand, key data 5 for deciphering the cipher in deciphering circuit 6 is supplied from key data memorizing circuit 4 to deciphering circuit 6. Deciphering circuit 6 deciphers coded letter 3 by using key data 5 and outputs the result as a normal letter. Normal letter 7 is output from normal letter output circuit as output normal letter 9. Here, coded letter input circuit 2 has a buffer function for processing input data at the deciphering circuit. For example, when input coded letter 1 is a serial data, coded letter input circuit 2 converts it into parallel data of a bit number, which is processed simultaneously by deciphering circuit 6. On the contrary, normal letter output circuit 8 converts the parallel data from deciphering circuit 6 into serial data again.

[0006]

Problem this invention intends to solve

In the above example, the key data is supplied from the key data memory circuit but long-time use of the same key data is not preferred for confidential communication. The reason for this is, when the same key data is used for a long time, an interceptor is provided with ample time and opportunity for collection and analysis of a sufficient sample of the communication letter and can discover the cipher key, so-called attacking of the known normal letter. Especially, when the algorithm of the cipher is published, discovery of the key data is easier so the key data must be able to be exchanged frequently.

[0007]

Naturally, the sender and recipient must be in synch for exchange of the key data, otherwise the recipient cannot decipher the coded letter. Key data is sent in various manners, for example, use of means other than the route for the coded letter, and this means offers higher safety. If communication of the coded letter is via wired transmission, the sender sends the cipher key data to the recipient in advance via physical means and the recipient thereby sets parameters for the cipher deciphering machine. In such a case, the 3rd party is deprived of the means of interception so that safety is high.

[0008]

However, if the sender and recipient are far away from each other and physical means other than the communication route is not available, the key data transmission must employ a route which can be intercepted by the 3rd party. In such a case, the risk of the key data being intercepted is high. Therefore, the key data is not renewed and the initial key data is used continuously by the key data memory circuit. That is, if the recipient is far away, new key data cannot be changed easily and the same key data must be used over a long period.

[0009]

This invention offers a data cipher device that is undecipherable to a 3rd party, even when the key data transmission occurs via a regular communication route.

[0010]

To solve the above conventional problem, this invention transmits multiple key data from sender to recipient via a regular communication route and yet, this invention makes deciphering of the key data difficult, even in the case of interception.

[0011]

Means for solving the problem

The data cipher device of this invention transmits key data as coded letter by a specific method and at an optional time for changing of the key data by the recipient. Upon receipt, the recipient evaluates whether it is key data coded by the said specific method or not and, when transmission of the key data is detected, the recipient renews the key data and, thereafter, deciphering is based on such new key data.

[0012]

Function

In the data cipher device of this invention, the key data is sent via the communication route for coded letter and it sends key data optionally via the coded letter communication route, even when the key data can only be sent via the coded letter communication route. Thereby, it makes deciphering of the cipher key data by a third party difficult.

[0013]

PRACTICAL EXAMPLES

Practical Example 1

Figure 1 is a block diagram of a data cipher device of a practical example of this invention. In the figure, 1 is an input coded letter, 2 is a coded letter input circuit, 3 is the coded letter, 4 is a key data memory circuit, 5 is the key data, 6 is a deciphering circuit, 7 is a normal letter, 8 is a normal letter output circuit, 9 is an output normal letter, 10 is a key data evaluation circuit and 11 is the renewed key data.

[0014]

Coded letter 3 is deciphered by deciphering circuit 4 and normal letter 7 is output as an output normal letter via normal letter output circuit 8. At the same time, normal letter 7 is supplied to key data evaluation circuit 10, too. The key data evaluation circuit detects specific data contained in normal letter 7 and when transmission of the key data is evaluated as being detected, renewed key data 11 is supplied to key data memory circuit 4. The key data of key data memory circuit 4 is renewed in such a manner and, thereafter, new key data is used for deciphering circuit 6. The sender renews its own ciphering key after sending the said key data, so that renewal of the key data is in synch between sender and recipient.

[0015]

In the above practical example, the function of the key data evaluation circuit is not specified, but the safety of the key data is dependent on the composition of the key data evaluation circuit.

[0016]

Figure 2 is a practical example of the key data evaluation circuit of this invention. In the figure, 12 is an "No. of bits 1" counting circuit that receives coded letter 3 and counts the number of bits 1 and bits 0 contained in coded letter 3, which is composed of 1 and 0. Numeral 13 is the number of bits 1 counted, 14a is the 1st count latch circuit, 15a is the latch output of the 1st count latch circuit, 14b is the 2nd count latch circuit, 15b is the latch output of the 2nd count latch output, 14c is the 3rd count latch circuit, 15c is the latch output of the 3rd count value latch output, 16 is a count collation circuit, 17 is a count agreement detection signal, 18 is the renewed key data edit circuit and 11 is the renewed key data. In Figure 2, renewed key data edit circuit 18 is normally in the disabled condition and normal letter 7 is input to the "No. of bits 1" counting circuit where the

number of bits 1 contained in a set normal letter block is counted and the result 13 is supplied to 1st count latch circuit 14a. Count value 13 is input to counting collation circuit 16 as 1st count latch output 15a. Normal letter 7 is input to "No. of bits 1" count circuit 12, one after another, and the number of bits 1 of each agreeing block is counted and the result transferred from 1st count latch circuit 14a to the 2nd count latch circuit 14b and 3rd count latch circuit 14c, in this order. Therefore, count latch outputs 15a, 15b and 15c, which are the outputs of these count latch circuits, always supply the count of the number of bits 1 contained in the newest 3 blocks of the received normal letter to count collation circuit 16. These count latch outputs 15a, 15b and 15c are always monitored by count collation circuit 16 and these counts are collated with a specific condition and, if agreement is detected, count agreement detection signal 17 is output to renewed key data edit circuit 18. Here, the specific condition is, for example, whether or not the sum of count latch outputs 15a, 15b and 15c is a specific numerical value. Renewed key data edit circuit 18 is in the disabled condition when count agreement detection signal 17 is input and it edits the bit correspondence of count latch outputs 15a, 15b and 15c in renewed key data edit circuit 18, according to a previously set rule. The renewed key data 11 is generated for renewal of the key data in key data memory circuit 4.

[0017]

EFFECT OF THE INVENTION

As shown above, this invention offers a means for sending a cipher key via a communication route for the coded letter and a means which cannot be intercepted by a third party as regards deciphering of the cipher key data itself and renewal time of the cipher key data. In this invention, key data is sent optionally via a coded letter communication route for frequent renewal of the key data and deciphering of the cipher key data by a third party who intercepts the said route is made difficult.

BRIEF EXPLANATION OF THE FIGURES

Figure 1 is one practical example of this invention.

Figure 2 is a block diagram of one practical example of this invention.

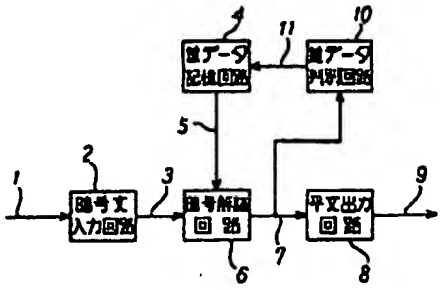
Figure 3 is a conventional practical example.

EXPLANATION OF THE CODES

1	input coded letter
2	coded letter input circuit
3	coded letter
4	key data memory circuit
5	key data
6	deciphering circuit
7	normal letter
8	normal letter output circuit
9	output normal letter
10	key data evaluation circuit
11	renewed key data
12	"No. of bits 1" counting circuit
13	count value
14a	1st count latch circuit
14b	2nd count latch circuit
14c	3rd count latch circuit
15a	1st count latch output
15b	2nd count latch output
15c	3rd count latch output
16	count collation circuit
17	count agreement detection signal
18	renewed key data edit circuit

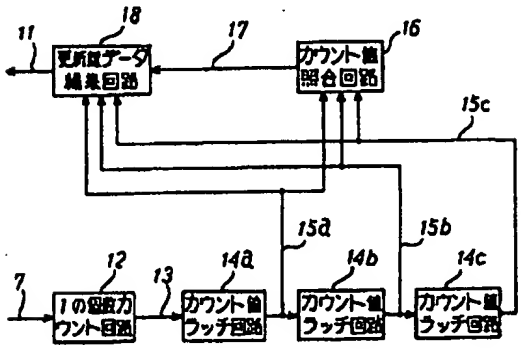
Key to Figure 1:
2 - coded letter input circuit
4 - key data memory circuit
6 - deciphering circuit
8 - normal letter output circuit
10 - key data evaluation circuit

Figure 1



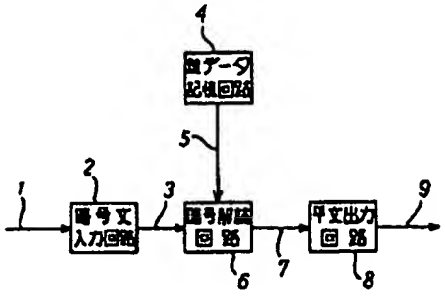
Key to Figure 2:
18 - renewed key data edit circuit
16 - count collation circuit
12 - "No. of bits 1" counting circuit
14a - 1st count latch circuit
14b - 2nd count latch circuit
14c - 3rd count latch circuit

Figure 2



Key to Figure 3:
4 - key data memory circuit
2 - coded letter input circuit
6 - deciphering circuit
8 - normal letter output circuit

Figure 3



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平4－297157

(43)公開日　平成４年(1992)10月21日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/28					
Ｇ０９Ｃ	1/00		7922－5L			
Ｈ０４Ｋ	1/00		7117－5K			
			7117－5K	Ｈ０４Ｌ	9／02	Ａ

審査請求　未請求　請求項の数２(全 ４ 頁)

(21)出願番号　特願平3－49700

(22)出願日　平成３年(1991)３月14日

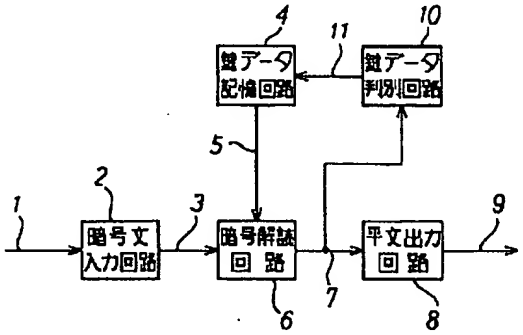
(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　三奈木　正純
鎌倉市上町屋325番地　三菱電機株式会社
鎌倉製作所内

(74)代理人　弁理士　高田　守　(外１名)

(54)【発明の名称】　データ暗号装置

(57)【要約】
【目的】　秘密鍵暗号通信系において、送信側と受信側が例えば長い距離で隔てられ、鍵データの配送を、第三者の傍受する通信路を経由する以外の手段のない場合に、第三者に配送される鍵データの解読及び鍵データの更新時期を解読することを困難ならしめる。
【構成】　受信側のデータ暗号装置において解読された平文データに含まれる特定の特徴を検出し、これによって鍵データの更新を送信側から受信側に知らせると共に、鍵データそのものも同時に上記特徴から抽出することによって、受信側で更新鍵データと更新時期を知るようにした。



1

【特許請求の範囲】

【請求項1】　秘密鍵暗号方式により暗号化された暗号文を受信し、これを解読して平文を得るデータ暗号装置において、暗号文を受信する暗号文入力回路と、暗号文を解読する為に必要な暗号鍵データを記憶する鍵データ記憶回路と、鍵データ記憶回路から出力される鍵データ及び前記暗号文入力回路の暗号文出力を入力され、暗号文を解読した結果を平文データとして出力する暗号解読回路と、暗号解読回路の平文データを入力されて、これを出力する平文出力回路と、前記暗号解読回路の平文データを分岐して入力されて新しい鍵データの更新時期と鍵データを判別し、これを前記鍵データ記憶回路へ供給する鍵データ判別回路とを備えたことを特徴とするデータ暗号装置。

【請求項2】　鍵データ判別回路として、”1”及び”0”よりなる平文データを一定のビット数のブロック毎に分割して入力し、各入力平文ブロックに含まれる1の個数をカウントする1の個数カウント回路と、前記1の個数カウント回路のカウント値を順次ラッチすることによって、複数の入力平文ブロックにおける1の個数を記憶するn段（nは正整数）のラッチ回路と、前記n段のラッチ回路の出力を加算し、その結果得られた数値が予め設定された数値と一致した場合にカウント値一致信号を発生するカウント値照合回路と、前記カウント値照合回路のカウント値一致検出信号を入力されることによってイネーブル状態になり、前記n段のラッチ回路のラッチ出力を編集して、これから新しい鍵データを生成する更新鍵データ編集回路を備えたことを特徴とする請求項1記載のデータ暗号装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、複数の鍵データを用いた暗号通信システムにおける暗号解読器に関するものである。

【0002】

【従来の技術】ディジタル通信の分野においては、情報源からの信号は、一般に”1”及び”0”の2値からなる数値列に変換され、この2値より、搬送信号を変調することによって無線または有線伝送路に送出され、目的地へ伝達される。情報源からの信号としては、例えば文字、音声や画像等があり、これらの情報源信号は伝送路上で容易に第三者の傍受が可能な状況にある。上記のように第三者が傍受可能な伝送路を使用して、情報を伝送する場合、秘匿性を有する情報源データについては情報源側で暗号化し、目的地の受信側でこれを暗号解読してもとの情報源からの信号を復元する、いわゆる暗号通信システムが構成される。

【0003】暗号通信システムとしては、様々な原理に基づくものが提案され、実用されているが、よく用いられる方式の一つに秘密鍵暗号方式と呼ばれるものがある。秘密鍵暗号方式では文字等の情報の順序を置き換える転置式、文字等の情報を他の文字等に置き換える換字式等が実用されている。これらの操作により、加工されて伝送路に送出される情報源からの情報は、どのような規則によって情報が加工されたを知らない第三者には解読できず、その規則を知っている目的地の受信側でのみ、解読可能とするものである。従って、上記秘密鍵暗号方式では、送信側と受信側が知っている。暗号化するために使用する規則すなわち転置や換字の対応表を、第三者に知られないように保護することが重要になる。転置や換字の対応表は鍵と呼ばれることから、上記の方式は秘密鍵暗号方式と呼ばれる。

【0004】図3は、秘密鍵暗号方式における、従来の暗号解読装置の例であり、図において1は入力暗号文、2は暗号文入力回路、3は暗号文、4は鍵データ記憶回路、5は鍵データ、6は暗号解読回路、7は平文、8は平文出力回路、9は出力平文である。

【0005】次に動作について説明する。入力暗号文1は暗号文入力回路2で受信され、暗号文3として、暗号解読回路6へ入力される。一方、暗号解読回路6において暗号を解読するための鍵データ5は、鍵データ記憶回路4から暗号解読回路6に供給される。暗号解読回路6は、鍵データ5を用いて、暗号文3を解読し、その結果を平文7として出力する。平文7は、平文出力回路から出力平文9として出力される。ここで暗号文入力回路2は入力データを暗号解読回路で処理するためのバッファの機能を有する。例えば、入力暗号文1がシリアルデータ形式の場合、暗号文入力回路2はこれを暗号文解読回路6が同時に処理するビット数からなるパラレルデータに変換する。また、平文出力回路8では逆に、暗号文解読回路6から出力されるパラレルデータを、再びシリアルデータに変換する機能を有する。

【0006】

【発明が解決しようとする課題】前記の実施例では、鍵データは鍵データ記憶回路から供給されるが、通信の秘匿性を確保するためには同一の鍵データを長く使用するのは好ましくない。同一の鍵データを使用して長期間にわたって通信を続けた場合、傍受者にとって、同一鍵による通信文の十分なサンプルを収集し、これを解析して暗号鍵を発見する、いわゆる既知平文攻撃等の十分な時間と機会を与えることになるからである。特に暗号のアルゴリズムが公開されている場合、鍵データの発見は一層容易になるため、鍵データは頻繁に交換できることが必要である。

【0007】さて、鍵データを交換する際には、当然送信側と受信側が同期して交換しなければ、受信側で暗号文を解読することができないことはいうまでもない、そこで、鍵データの配送はさまざまな方法でなされるが、例えば、暗号文を送受する通信路とは別の手段によって配送できれば、安全性が高い。暗号文の通信が有線によ

る電気通信で行われる系においては、予め送信側から暗号鍵データを交換する日時と新しい暗号鍵データを物理的な手段で受信側に配送し、受信側でこれらにもとづいて暗号解読機の各パラメータをセットする場合を考えると、第三者はこれを傍受する手段を持たず、高い安全性が確保できる。

【０００８】しかし、特に送信側と受信側の距離が著しく離れており、通信の伝送路以外の配送手段を持たない場合、即ち、鍵データを配送する物理的な手段を持たない場合は、鍵データの配送そのものも第三者の傍受可能な通信路によらざるを得ないことになる。この場合、鍵データを配送する通信路自体が第三者の傍受が可能であり、鍵データを解読される危険があるため、鍵データの更新は行われず、前記の実施例では、鍵データ記憶回路に初期設定された鍵データが連続的に使用されることになる。つまり、受信側が遠隔地にある場合は、新しい鍵データを容易に変更することができず、従って同一の鍵データを長期間使用せざるを得ないという課題があった。

【０００９】本発明は、鍵データの配送を通信の伝送路自体を使用して行って、かつ第三者の解読が不可能なデータ暗号装置を得ることにある。

【００１０】前記した従来の課題を対処するために、本発明は複数の鍵データを、送信側から受信側へ通信の伝送路を経由して配送しながら、傍受された場合にも鍵データの解読を困難とするものである。

【００１１】

【課題を解決するための手段】この発明に係るデータ暗号装置は、送信側が任意の時点で鍵データの変更を行う際に、鍵データを特定の方法で暗号文として暗号文の通信路から送信し、受信側ではこれを受信して、上記特定の方法で暗号化された鍵データであるかを判別し、鍵データの配送であることが検出された場合は、鍵データの更新を行い、これ以降の暗号解読は新しい鍵データによって行うようにするものである。

【００１２】

【作用】この発明におけるデータ暗号装置は、鍵データの配送を暗号文の通信路を経て行い、暗号文通信路以外に鍵データの配送を行うことができない通信系においても、暗号文通信路を経由して、任意に鍵データの配送を行うことによって、上記通信路を傍受する第三者による暗号鍵データの解読を困難とするものである。

【００１３】

【実施例】実施例１．図１はこの発明の一実施例を示すデータ暗号装置のブロック図であり、図において１は入力暗号文、２は暗号文入力回路、３は暗号文、４は鍵データ記憶回路、５は鍵データ、６は暗号解読回路、７は平文、８は平文出力回路、９は出力平文、１０は鍵データ判別回路、１１は更新鍵データである。

【００１４】暗号文３は、暗号解読回路４によって解読

され、平文７が、平文出力回路８を経て出力平文として出力されるが、平文７は同時に鍵データ判別回路１０へも供給される。鍵データ判別回路では、平文７に含まれる特定の情報を検出し、鍵データの配送であることを判別すると、検出された更新鍵データ１１を鍵データ記憶回路４に供給する。鍵データ記憶回路の鍵データは、このようにして更新され、これ以降の暗号解読回路４への鍵データは、新しいデータが使用される。送信側では、上記鍵データの配送を行ったあと自らの暗号化鍵も更新して、暗号化を行うため、送信及び受信側で同期した鍵データの更新が可能になる。

【００１５】さて上記の実施例では、鍵データ判別回路の動作について特定していないが、実施の鍵データの安全性は、鍵データ判別回路の構成によることはいうまでもない。

【００１６】図２は、この発明による鍵データ判別回路の一実施例である。図において、１２は暗号文３を入力されて、１及び０からなる暗号文３に含まれる１の個数をカウントするビット１個数カウント回路、１３はビット１個数カウント値、１４ａは第１のカウント値ラッチ回路、１５ａは第１のカウント値ラッチ回路のラッチ出力、１４ｂは第２のカウント値ラッチ回路、１５ｂは第２のカウント値ラッチ回路のラッチ出力、１４ｃは第３のカウント値ラッチ回路、１５ｃは第３のカウント値ラッチ回路のラッチ出力、１６はカウント値照合回路、１７はカウント値一致検出信号、１８は更新鍵データ編集回路、１１は更新鍵データである。図２において、更新鍵データ編集回路１８は通常ディスエーブル状態にあり、平文７は、ビット１個数カウント回路へ入力され、ここで一定の入力平文ブロックに含まれる１の個数がカウントされ、その個数カウント値１３が第一のカウント値ラッチ回路１４ａに供給され、カウント値１３は、第一のカウント値ラッチ出力１５ａとしてカウント値照合回路１６へ入力される。ビット１個数カウント回路１２には、次々に平文７が入力され、一致のブロック毎の１の個数がカウントされ、これは第一のカウント値ラッチ回路１４ａから、後段に位置する第二のカウント値ラッチ回路１４ｂ、第三のカウント値ラッチ回路１４ｃへと順に転送される。従って、これらのカウント値ラッチ回路の出力であるカウント値ラッチ出力１５ａ、１５ｂ、１５ｃは常に、受信した平文における最新の３ブロックに含まれる１の個数カウント値を、カウント値照合回路１６に供給する。カウント値照合回路１６では、これらのカウント値ラッチ出力１５ａ、１５ｂ及び１５ｃを常に監視し、これらのカウント値とある特定の条件との照合を行い、一致を検出すると、カウント値一致検出信号１７を更新鍵データ編集回路１８へ出力する。ここでカウント値の特定の条件としては、例えばカウント値ラッチ出力１５ａ、１５ｂ及び１５ｃの合計が特定の数値になることを照合する。更新鍵データ編集回路１８は、カ

5

ウント値一致検出信号１７を入力されるとイネーブル状態になり、更新鍵データ編集回路１８カウント値ラッチ出力１５ａ、１５ｂ及び１５ｃを予め設定された規則に従ってビット対応の編集を行い、更新鍵データ１１を発生して鍵データ記憶回路４の鍵データを更新する。

【００１７】

【発明の効果】以上のように、この発明によれば暗号文の送受に使用する通信路を用いて、暗合鍵を配送し、かつこれを傍受する第三者によって暗号鍵データそのものの解読及び暗号鍵データの更新時期を知り得ない手段を提供するものであり、暗号文通信路以外に鍵データの配送を行うことができない通信系においても、暗号文通信路を経由して、任意に鍵データの配送を行うことによって、頻繁に鍵データを更新し、上記通信路を傍受する第三者による暗号鍵データの解読を困難とする効果がある。

【図面の簡単な説明】

【図１】この発明の１実施例を示す図である。

【図２】この発明の１実施例の部分詳細ブロック図である。

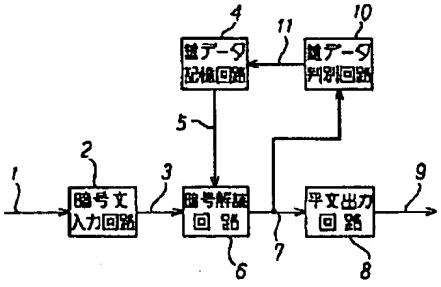
【図３】従来の実施例を示す図である。

【符号の説明】

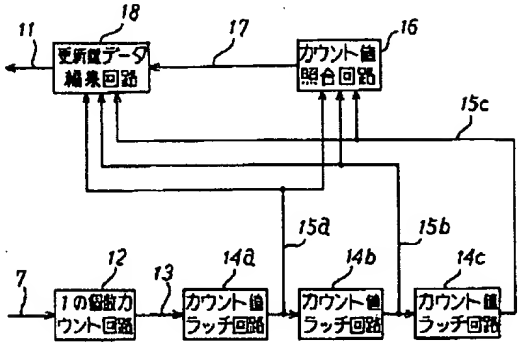
6

１　入力暗号文
２　暗号文入力回路
３　暗号文
４　鍵データ記憶回路
５　鍵データ
６　暗号解読回路
７　平文
８　平文出力回路
９　出力平文
１０　鍵データ判別回路
１１　更新鍵データ
１２　ビット１個数カウント回路
１３　個数カウント値
１４ａ　第１のカウント値ラッチ回路
１４ｂ　第２のカウント値ラッチ回路
１４ｃ　第３のカウント値ラッチ回路
１５ａ　第１のカウント値ラッチ出力
１５ｂ　第２のカウント値ラッチ出力
１５ｃ　第３のカウント値ラッチ出力
１６　カウント値照合回路
１７　カウント値一致検出信号
１８　更新鍵データ編集回路

【図１】



【図２】



【図３】